

## Edith Cowan University Research Online

---

Australian Digital Forensics Conference

Conferences, Symposia and Campus Events

---

2017

# Analysis of attempted intrusions: intelligence gathered from SSH Honeypots

Priya Rabadia

*Security Research Institute, Edith Cowan University, p.rabadia@ecu.edu.au*

Craig Valli

*Security Research Institute, Edith Cowan University, c.valli@ecu.edu.au*

Ahmed Ibrahim

*Security Research Institute, Edith Cowan University*

Zubair A. Baig

*Security Research Institute, Edith Cowan University, z.baig@ecu.edu.au*

Follow this and additional works at: <https://ro.ecu.edu.au/adf>

 Part of the [Information Security Commons](#)

---

### Recommended Citation

Rabadia, P., Valli, C., Ibrahim, A., & Baig, Z. A. (2017). Analysis of attempted intrusions: intelligence gathered from SSH Honeypots. DOI: <https://doi.org/10.4225/75/5a839e6d1d283>

DOI: [10.4225/75/5a839e6d1d283](https://doi.org/10.4225/75/5a839e6d1d283)

Rabadia, P., Valli, C., Ibrahim, A., & Baig, Z. (2017). Analysis of attempted intrusions: intelligence gathered from SSH Honeypots. *Paper presented in Valli, C. (Ed.). The Proceedings of 15th Australian Digital Forensics Conference 5-6 December 2017, Edith Cowan University, Perth, Australia.*

This Conference Proceeding is posted at Research Online.

<https://ro.ecu.edu.au/adf/173>

# ANALYSIS OF ATTEMPTED INTRUSIONS: INTELLIGENCE GATHERED FROM SSH HONEYPOTS

Priya Rabadia, Craig Valli, Ahmed Ibrahim, Zubair Baig  
Security Research Institute, Edith Cowan University, Perth, Western Australia  
p.rabadia@ecu.edu.au, c.valli@ecu.edu.au, ahmed.ibrahim@ecu.edu.au, z.baig@ecu.edu.au

## Abstract

*Honeypots are a defensive cyber security countermeasure used to gather data on intruder activities. By analysing the data collected by honeypots, mitigation strategies for cyberattacks launched against cyber-enabled infrastructures can be developed. In this paper, intelligence gathered from six Secure Shell (SSH) honeypots is presented. The paper is part of an ongoing investigation into analysing malicious activities captured by the honeypots. This paper focuses on the time of day attempted intrusions have occurred. The honeypot data has been gathered from 18th July 2012 until 13th January 2016; a period of 1,247 days. All six honeypots have the same hardware and software configurations, located on the same IPv4/24 subnet. Preliminary analysis of the data from all six hosts has been combined to show the number of attempted intrusions recorded by each honeypot and the top 20 countries attacking IP addresses have originated from. However, there is a variation in the number of attempted intrusions recorded on each of the six hosts. Findings from the research conducted suggest, there is a pattern of organised attempted intrusions from attacking IP addresses originating from China and Hong Kong during an 8am to 6pm working day. An additional investigation into the possible use of organised attacking workforces was conducted.*

**Keywords:** Cybersecurity, SSH, Secure Shell, Honeypots

## INTRODUCTION

Honeypots are decoy systems used to gather data on attempts made to gain unauthorised access to IT systems. There are three main types of honeypots that can be deployed. Firstly, a low-interaction honeypot is a system with minimal functionality and interaction with the actual honeypot. The configuration process is simple, with minimal maintenance required to sustain the honeypot. Secondly, a high-interaction honeypot. This system emulates a fully functional ‘real’ system; with an extensive configuration process. Due to the configuration of the system the maintenance and interaction required is demanding (Zemene & Avadhani, 2015). The final type of honeypot is a medium-interaction honeypot; it emulates some functionalities of a ‘real’ system. The configuration process is simpler than a high-interaction honeypot but the maintenance required is more demanding than a low-interaction honeypot (Zemene & Avadhani, 2015). An example of a medium-interaction honeypot is a Secure Shell (SSH) honeypot named Kippo (Desaster, 2013).

Kippo SSH is an application specific honeypot that imitates some functions that are exhibited by a ‘real’ SSH system to the attacker. SSH is designed to securely transmit data using a point to point encrypted tunnel. Kippo honeypots are designed to collect various data from attacks propagated against the SSH service (Rabadia & Valli, 2014). An open-source, python 2.7 based event-driven program called Twisted libraries (TwistedMatrixLabs, 2013) is deployed by the Kippo honeypot to imitate and project a legitimate SSH session to the attacker. Data for this study has been acquired from identically configured Kippo SSH honeypots, using Ubuntu 11 Long Term Support (LTS) servers as their base operating system. All the honeypots were located on inexpensive Virtual Private Servers (VPS) The six honeypots are referred to as: Bobtail, Bronx, Dugite, Goanna, Magpie and Mopoke. Three of the honeypots were based in the United States (Bobtail, Magpie and Mopoke) with the other three located in the Netherlands (Bronx, Dugite and Goanna.)

Preliminary analysis was conducted on the combined data from all six honeypots: the number of attempted intrusions recorded by each honeypot and the top 20 countries attacking Internet Protocol (IP) addresses have originated from. The focus of this research was on the time of day (24-hours) attempted intrusions had occurred. This paper is part of an ongoing investigation into data collected from Kippo SSH honeypots, with work conducted over the past five years 2012, 2013, 2014 and 2015 (Rabadia & Valli, 2014; Valli, 2012; Valli, Rabadia, & Woodward, 2013, 2015). An attempted intrusion is an unauthorised attempt to gain access or control of a honeypot.

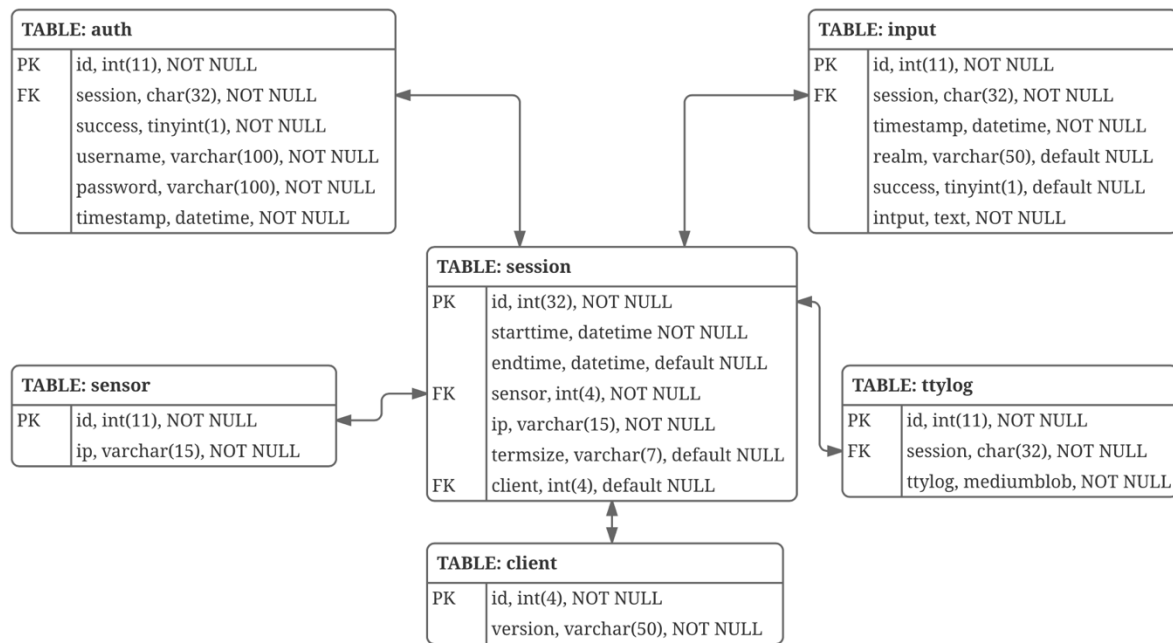


Figure 1 - MySQL database structure for Kippo honeypot, adapted from Valli, (2012)

## Overview of the Honeypot setup

Kippo honeypots are designed to collect data from attacker interaction with the emulated SSH service. The emulated SSH service is provided by an open-source, Python based event-driven program called Twisted (BruteForceLabs, 2011; TwistedMatrixLabs, 2013). Twisted provides the libraries that are utilised and deployed by Kippo honeypot to imitate a valid “encrypted” SSH session to an entity (BruteForceLabs, 2011). The Kippo honeypot also emulates a fake file system to present to the attacker, along with, false system reporting Kippo allows interaction with artefacts such as `/proc/cpuinfo` or `.bash_history` log file. The level of deception in the default setting is limited however, this functionality however, is able to be expanded and modified at will. For this experiment key elements were modified such as `/proc` entries and different bash file entries to deceive attackers.

The Kippo SSH honeypots are written in Python with a simple installation process. Source code was obtained from the [kippo.googlecode.com](http://kippo.googlecode.com) Wiki (Code.google.com, 2012). The setup for these particular systems used in the data collection was conducted as specified by the BruteForce Lab Guide (BruteForceLabs, 2011). This deviates from the original Kippo SSH documentation and uses the authbind daemon instead of `twistd` as the initial connecting daemon for the service. The configuration lets authbind handle the binding of the `twistd` as a non-root user to a low numbered TCP port and passes this to the Kippo daemon. This configuration has been found to be more consistent, reliable and secure during the conduct of the research project.

During the installation process a local MySQL database was configured securely to record all the interactions with the Kippo honeypots. Figure 1, reproduced from Valli (2012), shows the MySQL database structure used in the Kippo honeypots to record all the interactions.

After recording to the local MySQL database, these data were then transmitted to a centralised PostgreSQL SQL server that was running a Debian-Linux operating system (Valli et al., 2013). Communication is achieved using a Python extension that uses a PostgreSQL driver to connect to the SURFIDS system IDS logging server (IDS, 2013; SURFcrtIDS, 2013). The centralised logging server utilises the SURFIDS system for storing the data from the honeypots into an aggregated PostgreSQL database. The database has functions and tables specifically for the Kippo honeypots data. Since 2013 however, Elasticsearch has also been used to consume data from the honeypots in addition to recording with SQL.

In addition, on the honeypots that run Kippo the researchers also operate Dionaea (TheHoneyNetProject, 2011) and Glastopf (MushMushFoundation, 2011) which also report to the database instances, however these data are not used in this analysis for this research.

## PRELIMINARY ANALYSIS

Analysis conducted on the total number of attempted intrusions on each of the six honeypots and the top 20 countries attacking IP addresses have originated from is presented. An attempted intrusion is an unauthorised attempt to gain access or control of a honeypot. The data used in this study was collated from the sessions tables of the honeypot dataset, shown in Figure 1. The data used in this investigation has been collected from 18th July 2012 until 13th January 2016; this is a period of 1,247 days. Table 1 shows the number of attempted intrusions and the geolocations of the honeypots. A total of 5,554,680 attempted intrusions have been recorded, with the host known as Mopoke recording the most at 1,399,203 attacks. Host Goanna has received the least number of attacks at 520,250 as shown in Table 1.

Honeypot	Attempted Intrusions	Geolocation
Bobtail	934,966	United States
Bronx	1,319,381	Netherlands
Dugite	1,064,723	Netherlands
Goanna	520,250	Netherlands
Maggie	316,157	United States
Mopoke	1,399,203	United States
<b>Total</b>	<b>5,554,680</b>	

*Table 1: Number of attempted intrusions and the geolocation of the honeypots.*

Using the combined data from all six honeypots, the country of each attacking IP address session had been compiled using IP to ANS Mapping (TeamCymru, 2016) an open-source application that uses netcat. The top 20 countries attacking origin IPs was compiled and represented in Table 2. From 5,554,680 total attempted intrusions recorded; 31,596 unique attacking IP addresses have been identified attempting to gain unauthorized access to the six honeypots. Each host records the geolocation of the connections origin; however, this may not indicate the actual origin of the intruder attacking the hosts if the attacker is using a proxy. Data gathered from all six honeypots show ~64.47% of the recorded attacks originate from Chinese IP addresses followed by Romanian, Hong Kong, United States and France respectively as represented in Table 2.

	Countries	Attempted Intrusions
1	China	3,581,114
2	Romania	708,793
3	Hong Kong	427,209
4	United States	360,606
5	France	99,161
6	South Korea	90,983
7	Germany	34,253
8	Taiwan	19,906
9	Brazil	19,260
10	Ukraine	19,113
11	Russia	18,644
12	India	14,930
13	Indonesia	14,925
14	Czech Republic	13,999
15	Turkey	13,904
16	Japan	12,488
17	United Kingdom	12,066
18	Mexico	11,897
19	Canada	10,975
20	Italy	8,961

*Table 2: Top 20 originating countries of attacking IP addresses*

## INTELLIGENCE GATHERED

In this section, the time of day attempted intrusions occurred for each of the six honeypots is investigated, and the combined dataset is presented. RStudio Version 1.0.136 (RStudio, 2016) was used to examine the honeypot datasets. The start time of the attacking IP sessions was used as opposed to the end time, as the research investigates the number of attempted intrusions occurring during a 24-hour day. Next, the date part of the timestamps was stripped, leaving only the time segment. Each time segment was rounded to the nearest 15-minute interval. As hourly analysis would result in 24 data points and analysis conducted using 15 minute intervals resulted in 96 data points utilised. Allowing for a substantial data trend to be analysed, furthermore a reduced time interval could result in the data trend being hidden. The frequency of each 15-minute interval was compiled and depicted in Figure 2 to Figure 7. Once individual graphs for all six honeypots had been generated. The data from all six honeypots were combined and a graph was generated as shown in Figure 8.

Records of the interaction for each honeypot were stored in a combined MySQL database, the structure of which is shown in Figure 1. As the nature of the research requires an analysis of the timestamps; maintaining the timestamp throughout the data collection and data analysis phases of the research was essential for the purpose of validity. To ensure the integrity of the timestamp data recorded on all six hosts are consistent, the Network Time Protocol (NTP) is used to sync all six hosts to GMT +8 time.

### Attempted Intrusion Detected on the Honeypots

Figure 2 shows the time of day (24-hours format) using GMT+8 time as datum, for attempted intrusions that had occurred for the host known as Bobtail located in the United States. The highest recorded number of hits is at 04:15 with 11,495 attempted intrusions and the lowest number of hits recorded is at 14:45 with 9,122 hits. There is a significant decline in the number of attempted intrusions occurring after 12:00 until 00:15, with hits under 9,500. Whereas between 00:15 to 11:45 the number of intrusion attempts are above 10,000. This steep decline is clearly shown in Figure 2.

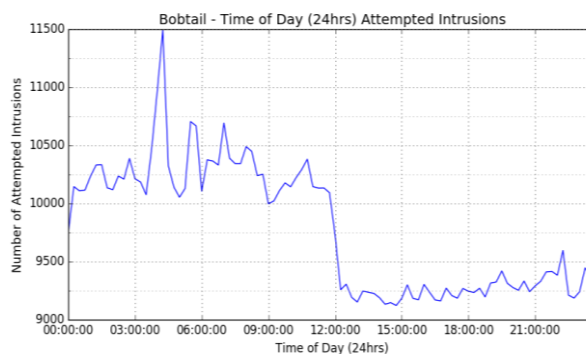


Figure 2: Time of day (24-hours) attempted intrusions occurred, for Bobtail.

Unlike Bobtail, the host known as Bronx shown in Figure 3, does not have a steep decline in the number of attempted intrusions recorded. Instead Bronx has a steady decline in the number of attempted intrusions throughout the day (24-hours). The highest recorded number of attempted intrusions is at 8:00 with 14,752 recorded and the lowest recorded at 21:45 with 12,899 hits. There is a steady decline in the number of hits recorded after 08:00 until 22:00, where the number attempted intrusions steadily increase again.

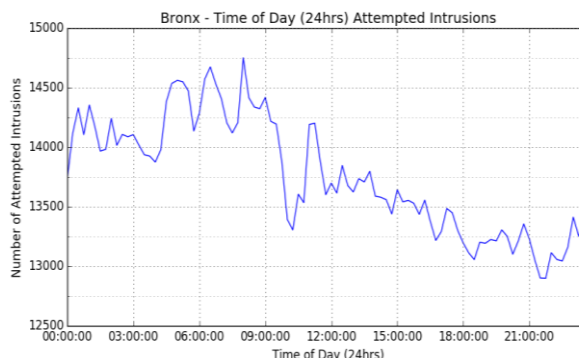


Figure 3: Time of day (24 hours) attempted intrusions occurred, for Bronx.

Similar to Bobtail (Figure 2), Dugite has a steep decline (Figure 4) in the number of attempted intrusions. The highest recorded attack is 12,222 at 7:30 and 14:00. With the lowest recorded hit at 17:00 with 10,186 attempted intrusions recorded. The steep decline in the number of attempted intrusions were recorded between 14:30 and 00:00, with around 10,500 and below. Whereas between 00:15 and 14:30 the number of hits were above 11,000. This is similar to the findings in from Bobtail.

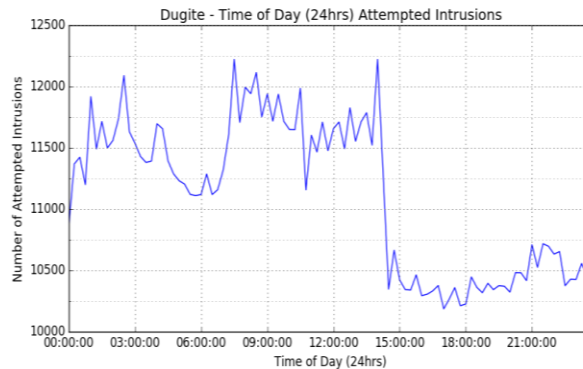


Figure 4: Time of day (24 hours) attempted intrusions occurred, for Dugite.

The host known as Goanna shown in Figure 5 has a steep decline in the number attempted intrusions similar to Figure 2 and Figure 4. The decline in the number of attempted intrusions starts 11:15 and continuous until 00:00. The number of attempted intrusions during this time are under 3,000. Most attempts occur between 00:15 and 11:00 with over 3,600 recorded attempts. The highest recorded number of attempted intrusions is 4,050 at 02:00, and the lowest number recorded is 2,718 at 17:15.

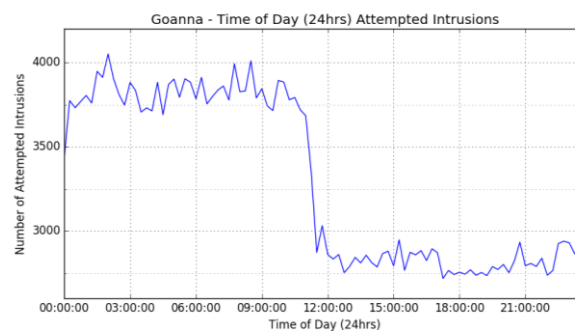


Figure 5: Time of day (24-hours) attempted intrusions occurred, for honeypot known as Goanna.

Figure 6 is from the Magpie host, it is similar to Bobtail, Dugite and Goanna as there is a steep decline in the number of attempted intrusions recorded. However, the number of attempted intrusions is mostly consistent throughout the day at around 5,500. There is a short decline from 20:45 until 23:45 with 4,700 recorded. The highest recorded attempted intrusions are at 8:45 with 6,371 hits recorded and the lowest at 23:00 with 4,529 hits recorded.

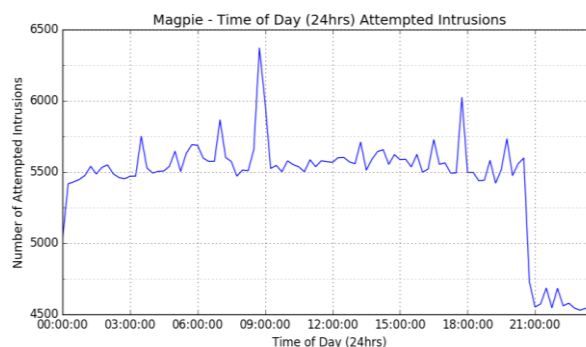


Figure 6: Time of day (24 hours) attempted intrusions occurred, for Magpie.

Host Mopoke shown in Figure 7, has the highest recorded number of attempted intrusions with 15,625 at 07:00, and the lowest number of hits recorded with 13,714 at 21:45. Mopoke, has similarities to Magpie, as there is a steep decline in attempted intrusions for a short time period compared to the other honeypots. The decline in the number of attempted intrusions recorded is from 19:30 until 00:00, with majority of the hits recorded below 14,000. While between 00:15 and 19:15 the number of hits are recorded above 14,500, showing Mopoke and Magpie had similar trends in the number of attempted intrusions.

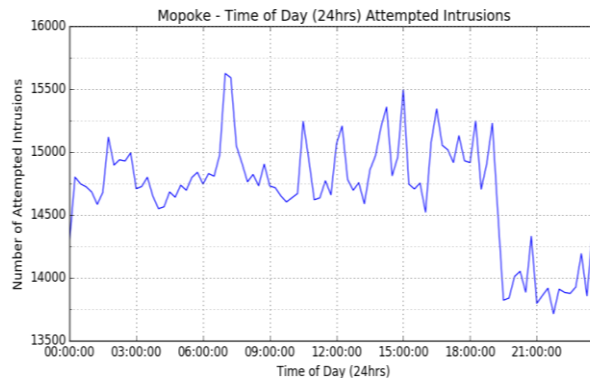


Figure 7: Time of day (24 hours) attempted intrusions occurred, for Mopoke.

Figure 8 is the combined data from all six honeypots; the mean line shows there is a steady decline in the number of attempted intrusions recorded. Whereas, the individual hosts aside from Bronx had a clear decline in the number of attempted intrusions recorded throughout the day (24-hours). The highest recorded number is at 8:00 with 60,219 and the lowest at 14:00 with 56,188 recorded. The mean line illustrates the number of attempted intrusions recorded increase during the hours between 00:15 and 09:00 and thereafter decreased.

## Summary

Findings from the data above suggest the number of attempted intrusions fluctuates as the day progresses. With Bobtail, Dugite and Goanna having similarities in a steep decline in the number of attacks from use times only. Whereas, Magpie and Mopoke only had a steep decline in the number of hits for a short period of time. Bronx and the mean from combined dataset show a steady decline in the number of attempted intrusions throughout the day.

Table 3 summaries the findings from all six honeypots including the combined dataset. As shown in Table 3, all means between 00:00-11:59 are higher than the means between 12:00-23:59 and the mean hits for a day. Additionally, all the peak numbers have occurred early in the timeline, while the minimum numbers have occurred later in the timeline.

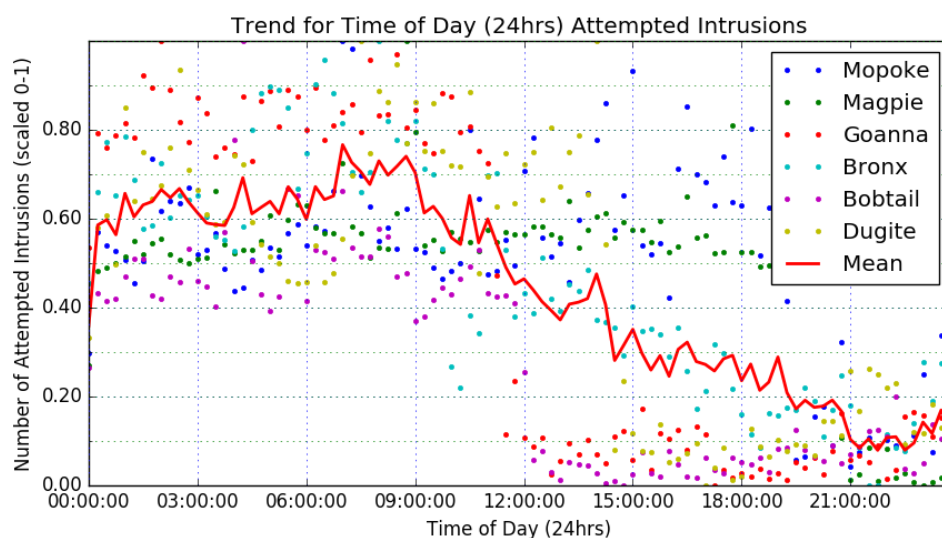


Figure 8: Time of day (24 hours) attempted intrusions occurred, for the combined hosts.

Table 3: Summary of the findings

Honeypot	Geolocation	Mean hits for a day	Mean between 00:00-11:59	Mean between 12:00-23:59	Peak Time	Peak Hits	Minimum Time	Minimum Hits
Bobtail	United States	9,780	10,287.29	9,272.71	04:15	11,495	14:45	9,122
Bronx	Netherlands	13,756.18	14,145.42	13,366.94	08:00	14,752	21:45	12,899
Dugite	Netherlands	11,115.53	11,547.75	10,683.31	07:30	12,222	17:00	10,186
Goanna	Netherlands	3,295.292	3,768.25	2,822.33	02:00	4,050	17:15	2,718
Magpie	United States	5,435.98	5,563.583	5,308.38	08:45	6,371	23:00	4,529
Mopoke	United States	14,689.52	14,800.25	14,578.79	07:00	15,625	21:45	13,714
Combined		58,072.5	58,407.23	57,737.77	08:00	60,219	14:00	56,188

Table 4: Summary of honeypot datasets excluding attacking IP addresses from China and Hong Kong

Honeypot	Geolocation	Total number of hits	Mean hits for a day	Mean between 00:00-11:59	Mean between 12:00-23:59	Peak Time	Peak Hits	Minimum Time	Minimum Hits
Bobtail	United States	341,777	3,560.18	3,502.94	3,617.42	11:45	5,521	05:15	1,962
Bronx	Netherlands	343,386	3,576.94	3,689.42	3,464.46	02:00	5,347	06:00	2,172
Dugite	Netherlands	205,860	2,144.38	2,178.15	2,110.6	11:45	3,325	07:45	283
Goanna	Netherlands	15,402	160.44	166.73	154.15	08:45	845	09:45	0
Magpie	United States	197,113	2,053.26	1,729.4	2,377.13	20:00	3,917	12:45	240
Mopoke	United States	463,093	4,823.89	4,535.54	5,143.76	12:00	8,120	07:15	2,812
Combined		1,566,631	16,319.07	16,111.29	16,526.85	23:45	18,858	01:30	12,485

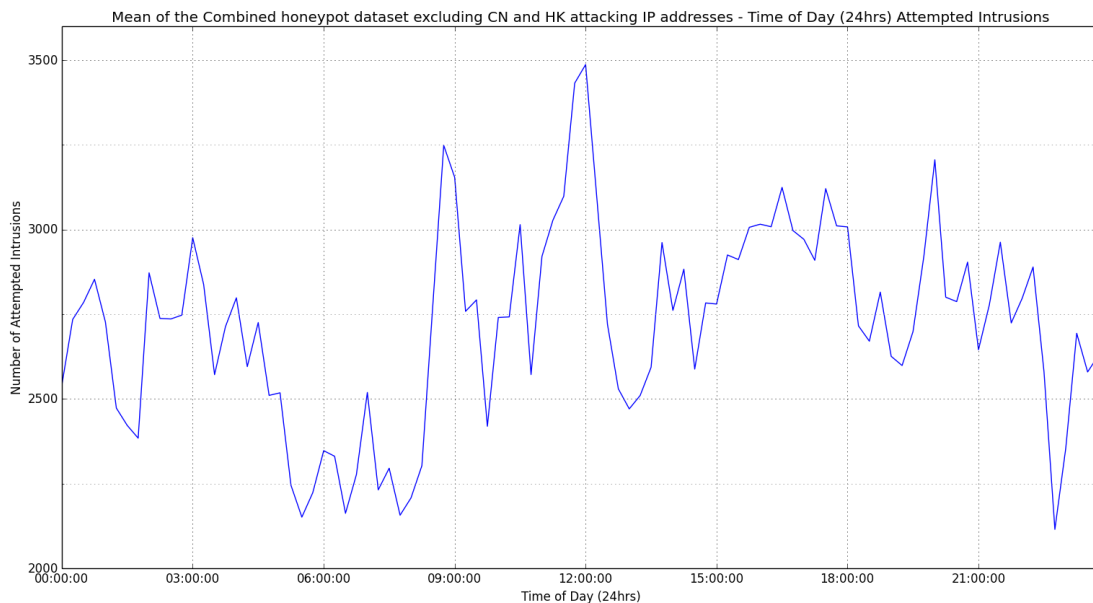


Figure 9: Combined dataset of mean time of day attempted intrusions have occurred excluding attacking IP addresses originating from China and Hong Kong.

## DISCUSSION

Preliminary analysis was conducted on the data collected from all six honeypots; the number of attempted intrusions recorded by each of the honeypots was presented. Mopoke recorded the most activity at 1,399,203. Among the top 20 countries where attacks originated (Table 2), IP address from China comprised about 65% of the attacks.

The mean from the complete datasets for all the honeypots show the mean between 00:00-11:59 is higher than the mean between 12:00-23:59. From the findings it is suggested that the geolocation of the honeypots may not



determine when attempted intrusions are carried out, as Bobtail (United States), Dugite (Netherlands) and Goanna (Netherlands) showed similar activities. However, Magpie and Mopoke were both located in the United States and similar activities had been identified. This mean indicates the global or distributed nature of these observed attacks.

The observation made from the data represented in the previous section suggest the number of attempted intrusion decrease as the day progresses. The honeypot datum is GMT+8 time. As shown in Table 2 attacking IP address originating from China and Hong Kong are first and third respectively. To verify whether there is a linkage between the decline in activity as the day progresses and attacking IP addresses originating from China and Hong Kong additional experiments had been conducted. IP addresses from China and Hong Kong had been removed from the individual honeypot datasets as well as the combined dataset.

Table 4 represents data from the honeypot datasets with attacking IP addresses originating from China and Hong Kong excluded. The honeypots located in the United States and the combined dataset have a higher mean for the hours between 12:00-23:59 as opposed to the mean for the hours between 00:00-11:59 and the mean for the whole day, unlike Table 3. Whereas, the honeypots located in the Netherlands have a higher mean for the hours between 00:00-11:59. The peaks are spread over the day, Table 3 shows peak occurring between 02:00-08:45, while Table 4 shows times between 02:00-20:00 and 02:00-23:45 when including the combined dataset. In Table 3, all minimum hits have occurred between 12:00-23:59 but Table 4 shows all minimum hits have occurred between 00:00-11:59 aside from Magpie with the minimum number of hits occurring at 12:45, suggesting the use of organised attacks.

*Table 5: Summary of honeypot datasets from attacking IP addresses from China*

Honeypot	Geolocation	Mean hits for a day	Mean between 00:00-07:59 & 17:00-23:59	Mean between 08:00-16:59	Mean between 00:00-08:29 & 17:30-23:59	Mean between 08:30-17:29	Mean between 00:00-08:59 & 18:00-23:59	Mean between 09:00-17:59	Mean between 00:00-07:59 & 18:00-23:59	Mean between 08:00-17:59
Bobtail	United States	5,731.99	5,819.28	5,586.5	5,882.92	5,480.44	5,898.52	5,454.44	5,879.93	5,524.88
Bronx	Netherlands	9,225.43	8,900.83	9,766.42	8,905.15	9,759.22	8,896.6	9,773.47	8,853.48	9,746.15
Dugite	Netherlands	7,733.6	7,745.08	7,714.44	7,823.62	7,583.56	7,880.12	7,489.39	7,831.86	7,596.03
Goanna	Netherlands	3,295.29	3,346.82	3,209.42	3,381.3	3,151.94	3,419.5	3,088.28	3,387.77	3,165.83
Magpie	United States	2,339.97	2,205.67	2,563.81	2,242.12	2,503.06	2,253.97	2,483.31	2,214.82	2,515.18
Mopoke	United States	9,137.96	9,239.28	8,969.08	9,243.05	8,962.81	9,236.08	8,974.42	9,241.25	8,993.35
Combined		37,303.27	37,256.13	37,381.83	37,243.62	37,402.69	37,235.85	37,415.64	36,961.95	37,781.13

The trends observed with the datasets including the attacking IP addresses from China and Hong Kong are not present when excluding these attacking IP addresses. Figure 9, depicts the mean for time of day and the number of attempted intrusions made for the combined dataset excluding attacking IP addresses originating from China and Hong Kong. Unlike figure 8, figure 9 does not have a distinct trend of a steady decline as the day progresses. There are many clear peaks and troughs throughout the day in figure 9 as opposed to figure 8. The trend of the number of attempted intrusions made decreases as the day progresses is present in the datasets including the Chinese and Hong Kong attacking IP addresses however it is not depicted in the datasets with these attacking IP addresses excluded.

Further investigation into the suggestion of organised attacker workforces being deployed by countries such as China has been conducted. The mean of the number of attempted intrusions occurring during the “average working day” ranging of hours between 08:00-17:59 were compared to the mean for the hours outside this range. By comparing the means of the number of attempted intrusions occurring between the “average working day” 08:00-17:59 and outside these specific hours of 00:00-07:59 then 18:00-23:59, it could be suggested organised attacks are being deployed within the working day. Table 5, shows the results from the analysis conducted. An “average working day” consisting of hours between 08:00-16:59, 08:30-17:29, 09:00-17:59 and 08:00-17:59. From the information shown in Table 5, only Bronx, Magpie and the combined dataset suggest presence of organised attacks being deployed. However, none of the means of the “average working day” for Bobtail, Dugite, Goanna and Mopoke are higher the means for the remainder of the day. Further investigation is needed

as Bronx and Magpie suggest the possible presence of organised attacks using workforce being deployed by countries such as China.

## CONCLUSION

The focus of this research was analysing the time of day attempted intrusions have occurred, the datum for this was GMT +8 time. The findings from this research show, the complete datasets from all six honeypots have a decline in the number of attacks as the day progressed through GMT +8 time. Three trends had been identified:

- A steep decline in the number of hits in the afternoon with the lower number of hits sustained between 00:00-11:59 GMT +8 time.
- A steep decline in the number of attacks, the decline in activity was for a shorter time period and much later in the day.
- A steady decline throughout the day.

Investigating further into the trends identified, all attacking IP addresses originating from China and Hong Kong were excluded. The observed trends in the complete dataset were not present in the dataset with the excluded attacking IP addresses. The honeypots located in the United States have a higher mean for the hours between 12:00-23:59, whereas the honeypots located in the Netherlands have a higher mean between 00:00-11:59. Unlike the complete datasets, all honeypots including the combined dataset had higher mean hits recorded between the hours of 00:00-11:59. Further investigation is needed to determine the significance of geolocation in the attempted honeypot intrusions. Upon the findings suggesting there is a linkage between time of day and attacking IP addresses originating from China and Hong Kong, additional investigation was conducted into the use of organised attacking work forces by countries such as China. The mean for the “average working day” was compared to the mean of hours outside the specify time. Analysing the results shown in Table 5, Bronx, Magpie and the combined dataset suggested the uses of organised attacking workforces being deployed as all four shifts had a high mean then the remainder on the day. However, the observation was not present in the remaining honeypots. Further research needs to be conducted as Bronx, Magpie and the combined dataset suggest the use of organised attacks during a working day by counties such as China.

## Future work

In future work, further analysis will be conducted on the Kippo SSH honeypot datasets. The time of day attacks have occurred for each of the top attacking countries including China and Hong Kong will be investigated which could yield an explanation in the decline of attacks as the day progresses. Also, data on the attacking IP addresses will be explored further, to identify if a distinct pattern for attacking IP addresses originating in the same geographical location is present. Analysis will also be conducted into suggestions of organised attacks during “business hours” workforces being deployed. Further investigation is needed to determine the significance of geolocation in attempted honeypot intrusions, this can be achieved by deploying honeypots in different geographical locations.

## REFERENCES

- BruteforceLabs. (2011). Installing Kippo SSH Honeypot on Ubuntu. Retrieved from <http://bruteforce.gr/installing-kippo-ssh-honeypot-on-ubuntu.html>
- Code.google.com. (2012). Kippo shows up in Metasploit. *SSH Honeypot* Retrieved from <https://code.google.com/p/kippo/issues/detail?id=48>
- Desaster. (2013). Kippo - SSH Honeypot. Retrieved from <https://github.com/desaster/kippo>
- IDS, S. (2013). SURFcert IDS. Retrieved from <http://ids.surfnet.nl/wiki/doku.php>
- MushMushFoundation. (2011). Glastopf. Retrieved from <http://mushmush.org/>
- NetworkWorkingGroup. (2006). RFC: The Secure Shell (SSH) Transport Layer Protocol.
- Rabadia, P., & Valli, C. (2014). *Finding evidence of wordlists being deployed against SSH Honeypots - implications and impacts*. Paper presented at the 12th Australian Digital Forensics Conference, Perth, W.A.
- RStudio. (2015). RStudio. Retrieved from <https://www.rstudio.com/>
- SURFcertIDS. (2013). SURFcert IDS. Retrieved from <http://ids.surfnet.nl/wiki/doku.php>

- TeamCymru. (2016). IP TO ASN MAPPING. Retrieved from <http://www.team-cymru.org/IP-ASN-mapping.html>
- TheHoneynetProject. (2011). Dionaea - catches bugs. Retrieved from <https://www.honeynet.org/project/Dionaea>
- TwistedMatrixLabs. (2013). What is Twisted? Retrieved from <http://twistedmatrix.com/trac/>
- Valli, C. (2012). *SSH: Somewhat Secure Host*. Paper presented at the Cyberspace Safety and Security, Melbourne Australia.
- Valli, C., Rabadia, P., & Woodward, A. (2013). *Patterns and Patter - An Investigation into SSH Activity Using Kippo Honeypots*. Paper presented at the Australian Digital Forensics Conference, Edith Cowan University.
- Valli, C., Rabadia, P., & Woodward, A. (2015). *Profile of Prolonged, Persistent SSH Attack on a Kippo Based Honeynet*. Paper presented at the Conference on Digital Forensics, Security and Law, Virginia, US.
- Zemene, M. S., & Avadhani, P. S. (2015, 10-13 Aug. 2015). *Implementing high interaction honeypot to study SSH attacks*. Paper presented at the Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on.